REMARKS

The present application was filed on February 14, 2002 with claims 1 through 14. Claims 1 through 14 are presently pending in the above-identified patent application.

In the Office Action, the Examiner rejected claims 1-4 and 9-14 under 35 U.S.C. §102(e) as being anticipated by Nelson et al. (United States Patent Application Publication Number 2003/0095663) and rejected claims 5-8 under 35 U.S.C. §103(a) as being unpatentable over Nelson et al. in view of Sowa et al. (United States Patent Application Publication Number 2002/0154781).

Independent Claims 1 and 11-14

Independent claims 1 and 11-14 were rejected under 35 U.S.C. §102(e) as being anticipated by Nelson et al. Regarding claims 1 and 13, the Examiner asserts that Nelson teaches loading a number of keys in a controller (i.e., client transmit key and client receive key), the number set so that a device connected to the wireless network can miss being re-authenticated for a predetermined number of the time periods and still communicate in a secure manner on the wireless network. In the Response to Arguments section of the present Office Action, the Examiner asserts that Nelson teaches that, "'once the new keys have been transmitted to all associated clients transmits with the latest generated transmit key, the access point switches over to its newly assigned transmit key;' therefore, should this switching over to the newly assigned transmit key take place as it is expected to, no re-authentication is necessary to gain access to the network."

Applicants note that Nelson describes the process of authentication and reauthentication in paragraph 23. In particular, Nelson teaches that,

> in a shared key environment, the access point confirms that all connected clients return a message using the most recent client transmit key before beginning to transmit on the most recent client receive key. Alternatively, the access point may use a fixed number of duplicate key messages, i.e., retries, in the absence of positive acknowledgement from the client that the key messages have been received and processed. ***Once all clients are on the correct WEP key pair, signal exchanges are continued.***
> (Paragraph 0023; emphasis added.)

Nelson also teaches that,

> first, a network session is initiated by a wireless client via an access point. That initialization is secured through the TLS or other suitable protocol. Second, the client is authenticated by the network authentication server using the 802.1x authentication format. Third, *the access point creates a pair of keys and marks one as a client* ***receive key*** *and the other as a* ***client transmit*** *key.* Fourth, the access point delivers the key pair to a client via 802.1x key list or register. The capacity of the list or register is selectable. The access point may generate individual key pairs for each client with which it is associated. However, for efficiency purposes, each access point may generate a key pair usable by all clients associated with that access point. Fifth, each client receiving a key pair then transmits to the access point using the most recent transmit key. Finally, ***once the new keys have been transmitted to all associated clients transmits with the latest generated transmit key, the access point switches over to its newly assigned transmit key (the receive key for the client(s))***. The process of newly generated key pairs is periodically repeated as designed. Alternatively, the transition to the newly assigned pair may be time-dependent. In that case, a client that fails to switch over to the new key pair would be ***required to re-authenticate to gain access to the network***.
> (Paragraph 0014; emphasis added.)

The Examiner cites paragraph 0014 of Nelson to assert that, should the switching over to the newly assigned transmit key take place as it is expected to, ***no re-authentication is necessary*** to gain access to the network. Applicants note that, since "*no re-authentication is necessary*" in the Examiner's example, then the client is not missing a re-authentication; therefore, Nelson, in this example, is ***not*** addressing the situation wherein a re-authentication is missed. Independent claims 1 and 12-14 require loading a number of keys in a controller, the number set so that a device connected to the wireless network *can* ***miss being re-authenticated*** *for a predetermined number of the time periods and still communicate in a secure manner on the wireless network.* Independent claim 11 requires loading a plurality of keys, the number set so that a device connected to the wireless network *can* ***miss being re-authenticated*** *for a predetermined number of the time periods and still communicate in a secure manner on the wireless network.*

Thus, Nelson et al. do not disclose or suggest loading a number of keys, the number set so that a device connected to the wireless network can miss being re-authenticated for a predetermined number of the time periods and still communicate in a secure manner on the

wireless network, as required by independent claims 1 and 11-14.

Additional Cited References

Sowa was also cited by the Examiner for its disclosure of, for example, loading a fixed key, and loading at least one additional key, wherein the number of keys comprises the fixed key and the at least one additional key (page 2, paragraph 0026-0031). Sowa, however, does not address the issue of loading a number of keys, wherein the number is set so that a device connected to the wireless network can miss being re-authenticated for a predetermined number of the time periods and still communicate in a secure manner on the wireless network.

Thus, Sowa et al. do not disclose or suggest loading a number of keys, the number set so that a device connected to the wireless network can miss being re-authenticated for a predetermined number of the time periods and still communicate in a secure manner on the wireless network, as required by independent claims 1 and 11-14.

Dependent Claims 2-10

Dependent claims 1-4 and 9-10 were rejected under 35 U.S.C. §102(e) as being anticipated by Nelson et al. and claims 5-8 were rejected under 35 U.S.C. §103(a) as being unpatentable over Nelson et al. in view of Sowa et al.

Claims 2-10 are dependent on claim 1 and are therefore patentably distinguished over Nelson et al. and Sowa et al., alone or in combination, because of their dependency from independent claim 1 for the reasons set forth above, as well as other elements these claims add in combination to their base claim.

All of the pending claims, i.e., claims 1-14, are in condition for allowance and such favorable action is earnestly solicited.

If any outstanding issues remain, or if the Examiner has any further suggestions for expediting allowance of this application, the Examiner is invited to contact the undersigned at the telephone number indicated below.

The Examiner's attention to this matter is appreciated.

Respectfully submitted,

Kevin M. Mason

Date: May 15, 2006

Kevin M. Mason
Attorney for Applicants
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06824
(203) 255-6560